

## Setting up the OPAM Audit Module

OPAM logs all security events as auditable data which can be used to get detailed insight of Privileged Account management and thus helps refine and effectively manage their usage.

OPAM can be configured to store audit data in either of the below mentioned repositories.

- File - Audit info are stored in the file system on the OS
- Database - Audit event info is pushed to a Database.

### **Note:**

- None of the audit stores are configured OOTB.
- BI Publisher reporting can be leveraged if the Audit repository is a database

We are going to look at a scenario where a Database can be used to store the audit event information

### **High Level steps**

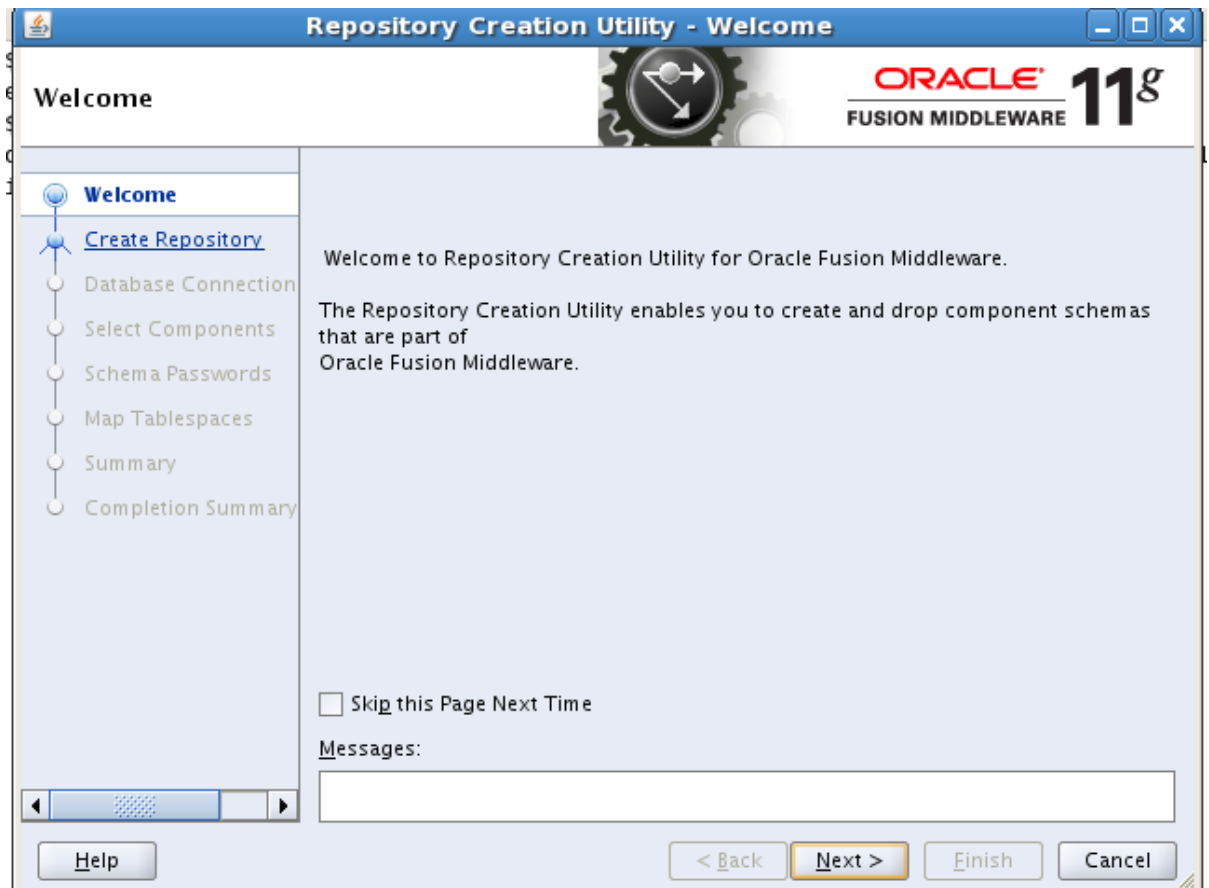
- Create Audit Schema using RCU  
([http://docs.oracle.com/cd/E29505\\_01/core.1111/e10043/audpolicy.htm#BABHGBAH](http://docs.oracle.com/cd/E29505_01/core.1111/e10043/audpolicy.htm#BABHGBAH))
- Create JDBC Data Source in the OPAM Weblogic Server (providing Audit Schema details)
- Configure OPAM to use Database centric audit logging
- Install BI Publisher
- Configure BI Publisher with Audit Data Store details
- Configure OPAM reports with BI Publisher

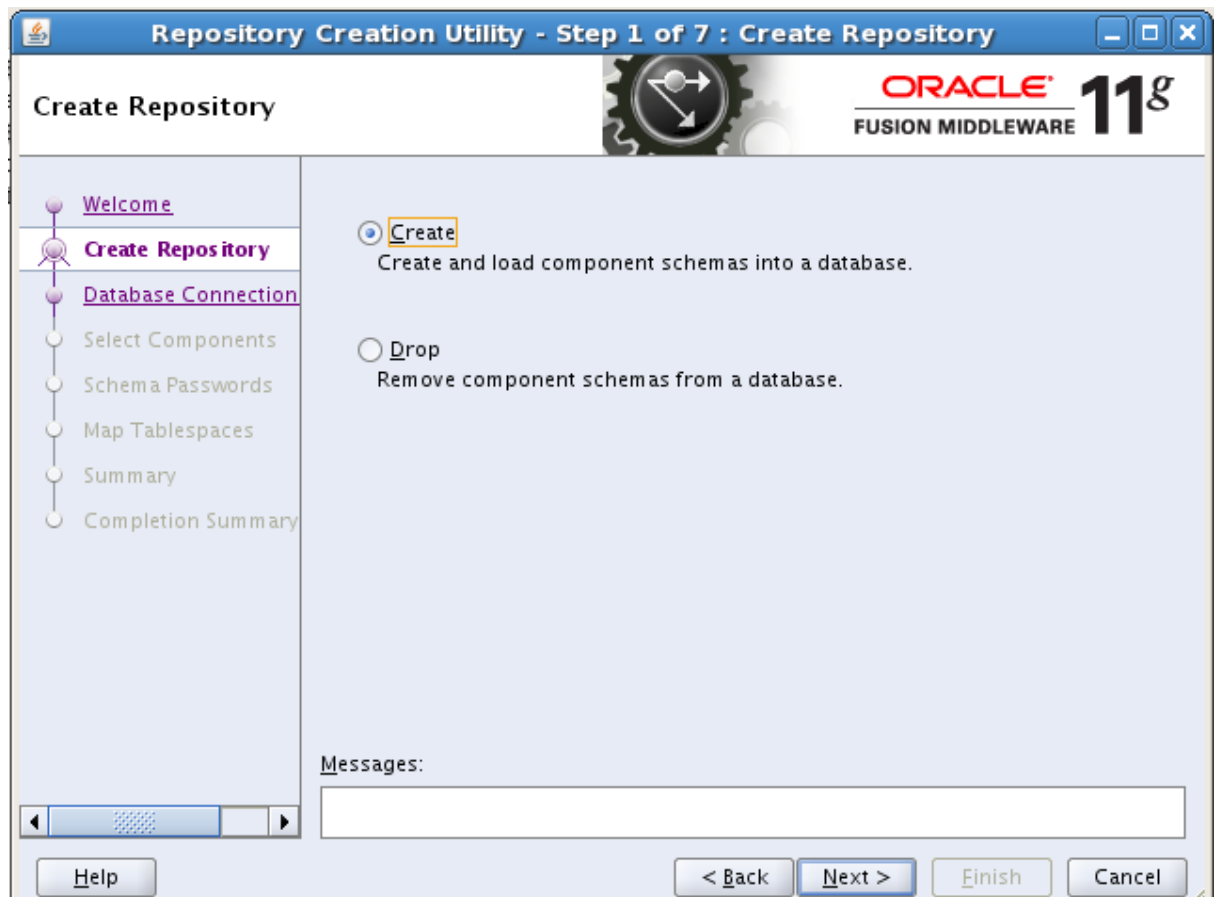
### **1. Create Audit Schema using RCU**

Execute RCU

```
cd /u01/R2_PS2_Installables/rcuHome/bin
```


```
oracle@localhost:/u01/R2_PS2_Installables/rcuHome/bin
File Edit View Terminal Tabs Help
[oracle@localhost bin]$ pwd
/u01/R2_PS2_Installables/rcuHome/bin
[oracle@localhost bin]$ ./rcu
```





Repository Creation Utility - Step 2 of 7 : Database Connection Details

### Database Connection Details



- Welcome
- Create Repository
- Database Connection**
- Select Components
- Schema Passwords
- Map Tablespaces
- Summary
- Completion Summary

Database Type:

Host Name:   
For RAC database, specify VIP name or one of the Node name as Host name.  
For SCAN enabled RAC database, specify SCAN host as Host name.

Port:

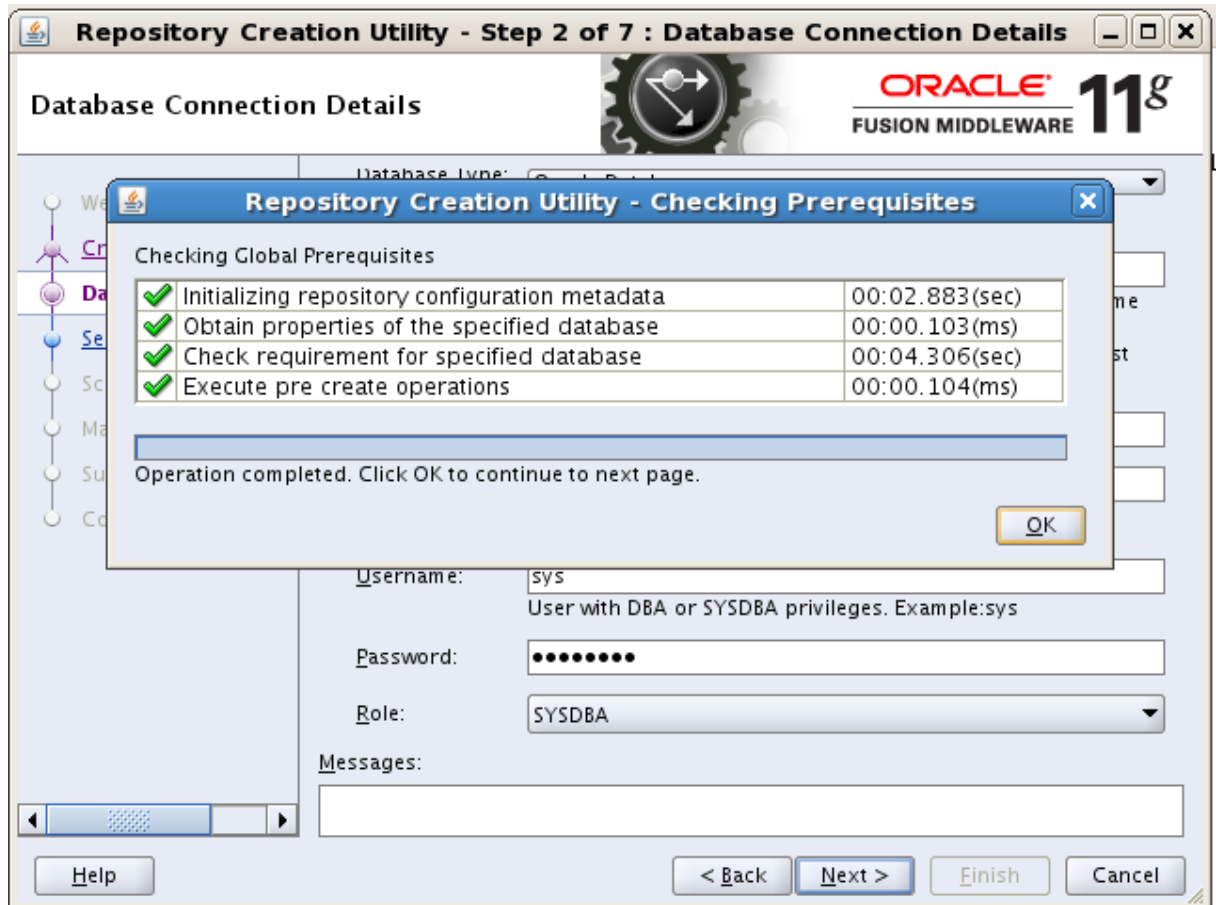
Service Name:

Username:   
User with DBA or SYSDBA privileges. Example:sys

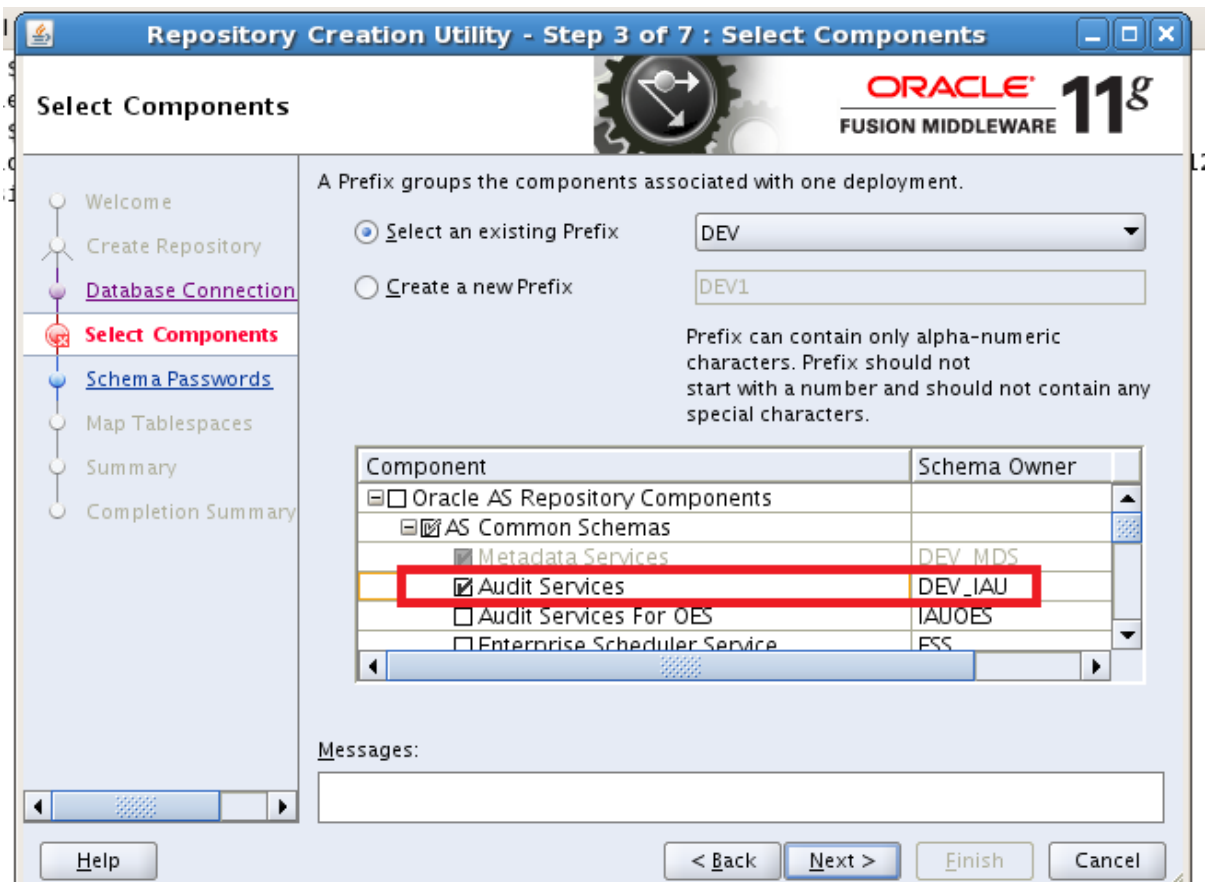
Password:

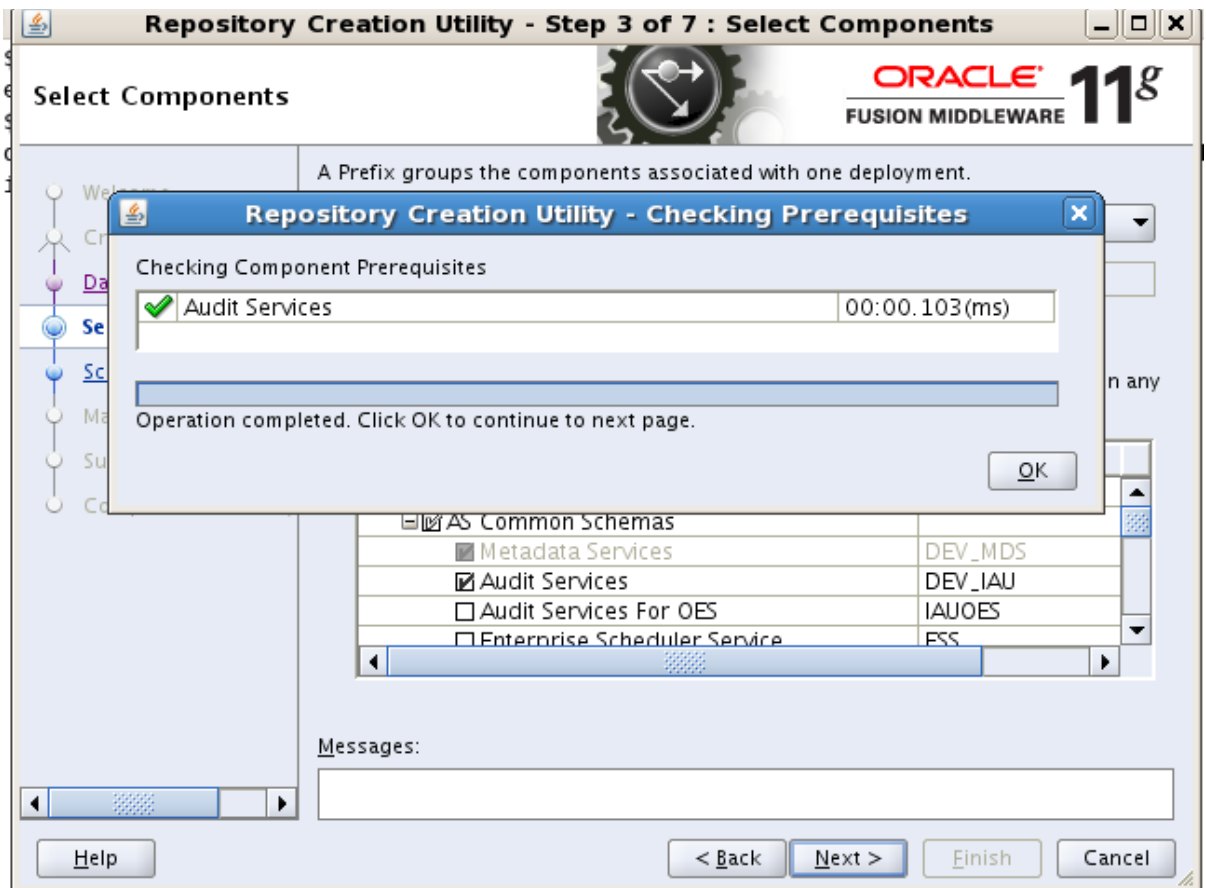
Role:

Messages:



**Select Audit Services**





Schema Passwords

Welcome
Create Repository
Database Connection
Select Components
Schema Passwords
Map Tablespaces
Summary
Completion Summary

Please enter the passwords for the main and additional (auxiliary) schema users. Password can contain alphabets, numbers and the following special characters: \$, #, \_ . Password should not start with a number or a special character.

☒ Use same passwords for all schemas

Password

Confirm Password

☐ Use main schema passwords for auxiliary schemas
☐ Specify different passwords for all schemas

Component	Schema Owner	Schema Password	Confirm Password
Audit Services	DEV_IAU		
Auxiliary Schema	DEV_IAU_APPEND		
Auxiliary Schema	DEV_IAU_VIEWER		

Messages:

Help

< Back

Next >

Finish

Cancel



Map Tablespaces

- Welcome
- Create Repository
- Database Connection
- Select Components
- Schema Passwords
- Map Tablespaces**
- Summary
- Completion Summary

Choose tablespaces for the selected components. The default and temporary tablespaces are specified in the table below. To create new tablespaces or modify existing tablespaces click the 'Manage Tablespaces' button.

Component	Schema Owner	Default Tablespace	Temp
Audit Services	DEV_IAU	*DEV_IAS_IAU	DEV_I

\* Default tablespaces (specified in the configuration files) are to be created upon confirmation.

[Manage Tablespaces](#)

Messages:

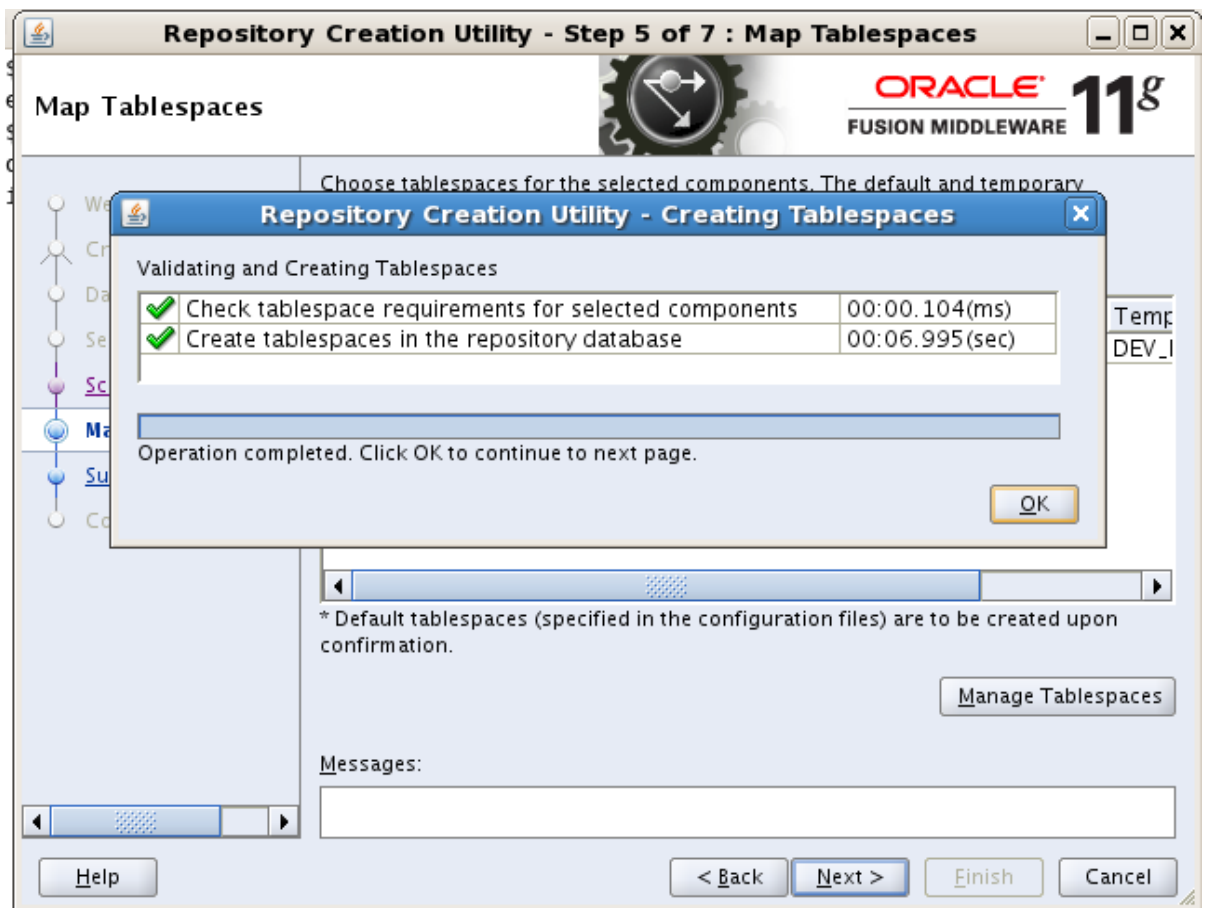
Help

< Back

Next >

Finish

Cancel



Repository Creation Utility - Step 6 of 7 : Summary

Summary

Welcome

Create Repository

Database Connection

Select Components

Schema Passwords

Map Tablespaces

Summary

Completion Summary

Database details:

Host Name: localhost

Port: 1521

Service Name: ORCL

Connected As: sys

Operation: Create

Prefix for (prefixable) Schema Owners:DEV

Component	Schema Owner	Tablespace Type	Tablespace Name
Audit Services	DEV_IAU	Default	DEV_IAS_IAU
		Temp	DEV_IAS_TEMP
		Additional	None

ORACLE 11g

FUSION MIDDLEWARE

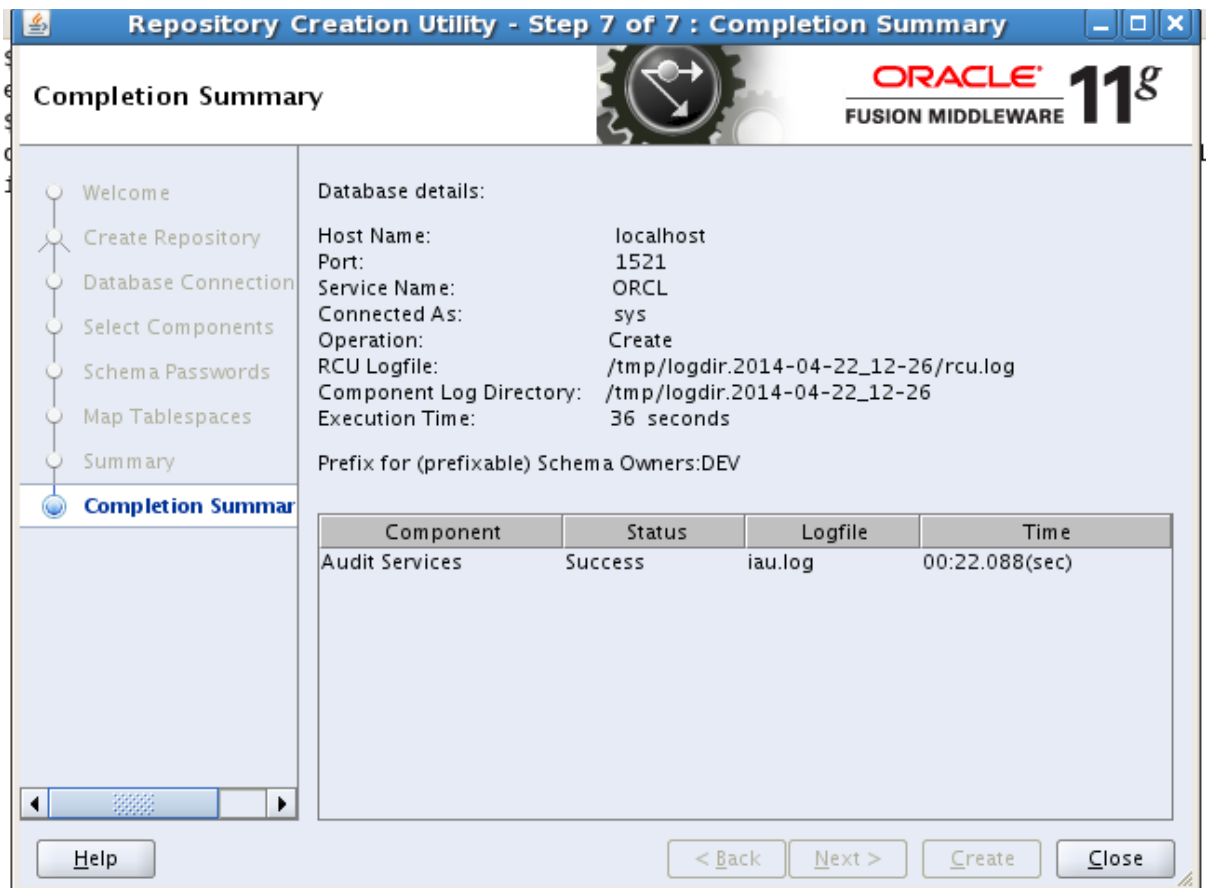
Help

< Back

Next >

Create

Cancel



## 2. Create JDBC Data Source in the OPAM Weblogic Server

We will configure and deploy the JDBC data source on both **OPAM Admin** and **managed servers**

Start OPAM Weblogic Admin and managed servers (if not already running) and then initiate Data Source configuration using steps below

ORACLE WebLogic Server® Administration Console

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: opam\_domain

**Change Center**  
View changes and restarts  
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

**Domain Structure**  
opam\_domain  
├── Environment  
├── Deployments  
├── Services  
│ ├── Messaging  
│ └── **Data Sources**  
├── Persistent Stores  
├── Foreign JNDI Providers  
├── Work Contexts  
├── XML Registries  
├── XML Entity Caches  
├── JCOM  
├── Mail Sessions  
└── File T3

**How do I...**  
• Create JDBC generic data sources

**Summary of JDBC Data Sources**  
Configuration Monitoring

A JDBC data source is an object bound to the JNDI tree that provides database connectivity through a pool of JDBC connections. Applications can look up a data source on the JNDI tree and then borrow a database connection from a data source.

This page summarizes the JDBC data source objects that have been created in this domain.

[Customize this table](#)

**Data Sources (Filtered - More Columns Exist)**  
New Delete Showing 1 to 2 of 2 Previous | Next

<input type="checkbox"/>	Name ↕	Type	JNDI Name	Targets
<input type="checkbox"/>	opamDS	Generic	jdbc/OPAMDS	opam_server1
<input type="checkbox"/>	opss-DBDS	Generic	jdbc/OPSSDBDS	AdminServer, opam_server1

New Delete Showing 1 to 2 of 2 Previous | Next

Make sure that the JNDI name for the Data Source is ***jdbc/AuditDB***

## Create a New JDBC Data Source

Back

Next

Finish


Cancel

### JDBC Data Source Properties

The following properties will be used to identify your new JDBC data source.

\* Indicates required fields

What would you like to name your new JDBC data source?

 \* Name:

OPAM Audit DS

What JNDI name would you like to assign to your new JDBC Data Source?

 JNDI Name:

jdbc/AuditDB

What database type would you like to select?

Database Type:

Oracle

Back

Next

Finish

Cancel

s

Create a New JDBC Data Source

Back

Next

Finish

Cancel

JDBC Data Source Properties

The following properties will be used to identify your new JDBC data source.

Database Type:

Oracle

What database driver would you like to use to create database connections? Note: \* indicates that the driver is explicitly supported by Oracle WebLogic Server.

Database Driver:

\*Oracle's Driver (Thin) for Instance connections; Versions:9.0.1 and later

Back

Next

Finish

Cancel

## Default Selections

Create a New JDBC Data Source

Back

Next

Finish

Cancel

Transaction Options

You have selected non-XA JDBC driver to create database connection in your new data source.

Does this data source support global transactions? If yes, please choose the transaction protocol for this data source.

☒ Supports Global Transactions

Select this option if you want to enable non-XA JDBC connections from the data source to participate in global transactions using the *Logging Last Resource* (LLR) transaction optimization. Recommended in place of Emulate Two-Phase Commit.

☐ Logging Last Resource

Select this option if you want to enable non-XA JDBC connections from the data source to emulate participation in global transactions using JTA. Select this option only if your application can tolerate heuristic conditions.

☐ Emulate Two-Phase Commit

Select this option if you want to enable non-XA JDBC connections from the data source to participate in global transactions using the one-phase commit transaction processing. With this option, no other resources can participate in the global transaction.

☒ One-Phase Commit

Back

Next

Finish

Cancel

Create a New JDBC Data Source

Back Next Finish Cancel

---

**Connection Properties**  
Define Connection Properties.

---

What is the name of the database you would like to connect to?

**Database Name:**

---

What is the name or IP address of the database server?

**Host Name:**


---

What is the port on the database server used to connect to the database?

**Port:**

---

What database account user name do you want to use to create database connections?

**Database User Name:**   **The Audit Schema user we just create using RCU**

---

What is the database account password to use to create database connections?

**Password:**

**Confirm Password:**

---

Back Next Finish Cancel

Test the connection



✔ Connection test succeeded.

## Create a New JDBC Data Source

### Test Configuration

[Back](#)

Next

Finish

Cancel

### Test Database Connection

Test the database availability and the connection properties you provided.

What is the full package name of JDBC driver class used to create database connections in the connection pool?

(Note that this driver class must be in the classpath of any server to which it is deployed.)

Driver Class Name:

```
oracle.jdbc.OracleDriver
```

What is the URL of the database to connect to? The format of the URL varies by JDBC driver.

**URL:**

jdbc:oracle:thin:@localh

What database account user name do you want to use to create database connections?

Database User Name:

dev\_iau

What is the database account password to use to create database connections?

(Note: for secure password management, enter the password in the Password field instead of the Properties field below)

**Password:**

Settings for OPAM Audit DS

Configuration

**Targets**

Monitoring

Control

Security

Notes

Save

This page allows you to select the servers or clusters on which you would like to deploy this JDBC data source.

Servers

☒ AdminServer

☒ opam\_server1

Save

Messages

✔ All changes have been activated. No restarts are necessary.

Summary of JDBC Data Sources

Configuration

Monitoring

A JDBC data source is an object bound to the JNDI tree that provides database connectivity through a pool of JDBC connections. Applications can look up a data source on the JNDI tree and then borrow a database connection from a data source.

This page summarizes the JDBC data source objects that have been created in this domain.

[Customize this table](#)

Data Sources (Filtered - More Columns Exist)

New ▼Delete

Showing 1 to 3 of 3Previous | Next

<input type="checkbox"/> Name ↕	Type	JNDI Name	Targets
<input type="checkbox"/> OPAM Audit DS	Generic	jdbc/OPAMAudit	opam_server1
<input type="checkbox"/> opamDS	Generic	jdbc/OPAMDS	opam_server1
<input type="checkbox"/> opss-DBDS	Generic	jdbc/OPSSDBDS	AdminServer, opam_server1

New ▼Delete

Showing 1 to 3 of 3Previous | Next

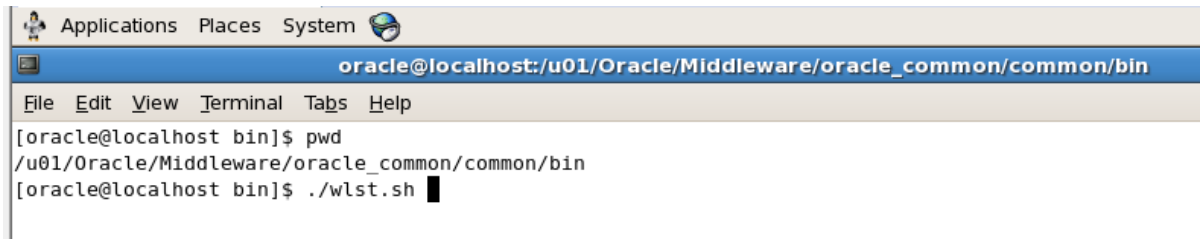
### 3. Configure OPAM to use Database centric audit logging

By Abhishek Gupta

Initiate WLST

```
cd /u01/Oracle/Middleware/oracle_common/common/bin
```

```
./wlst.sh
```

A screenshot of a Linux terminal window. The title bar shows 'Applications Places System' and a terminal icon. The window title is 'oracle@localhost:/u01/Oracle/Middleware/oracle\_common/common/bin'. The menu bar includes 'File Edit View Terminal Tabs Help'. The terminal content shows the user 'oracle@localhost' in the 'bin' directory. They run 'pwd' which returns '/u01/Oracle/Middleware/oracle\_common/common/bin'. Then they run './wlst.sh' and the prompt changes to 'wls:/opam\_domain/serverConfig>'.

```
oracle@localhost:/u01/Oracle/Middleware/oracle_common/common/bin
File Edit View Terminal Tabs Help
[oracle@localhost bin]$ pwd
/u01/Oracle/Middleware/oracle_common/common/bin
[oracle@localhost bin]$ ./wlst.sh
```

On the WLST console, execute below commands

```
connect('weblogic','password123','localhost:9001')
```

```
wls:/offline> connect('weblogic','password123','localhost:9001')
Connecting to t3://localhost:9001 with userid weblogic ...
Successfully connected to Admin Server 'AdminServer' that belongs to domain 'opam_domain'.

Warning: An insecure protocol was used to connect to the
server. To ensure on-the-wire security, the SSL port or
Admin port should be used instead.

wls:/opam_domain/serverConfig>
```

As of now, we will configure OPAM for MAXIMUM AUDIT logging level

```
setAuditPolicy(filterPreset='All')
```

```
wls:/opam_domain/serverConfig> setAuditPolicy(filterPreset='All')
Location changed to domainRuntime tree. This is a read-only tree with DomainMBean as the root.
For more help, use help(domainRuntime)

Audit Policy Information updated successfully
Server need to be restarted for the changes to take effect
wls:/opam_domain/serverConfig>
```

Configure DB as the audit repo

setAuditRepository(switchToDB='true')

```
Server need to be restarted for the changes to take effect
wls:/opam_domain/serverConfig> setAuditRepository(switchToDB='true')

Audit Repository Information updated
Server need to be restarted for the changes to take effect
wls:/opam_domain/serverConfig>
```

Restart OPAM Admin and Managed servers